L'insostenibile inaffidabilità della complessità

(424)—Un ben documentato "Io l'avevo detto" di Cassandra; l'eccesso di complessità può compromettere in maniera catastrofica il nostro…

Cassandra Crossing/ L'insostenibile inaffidabilità della complessità

(424)—Un ben documentato "Io l'avevo detto" di Cassandra; l'eccesso di complessità può compromettere in maniera catastrofica il nostro mondo connesso.

8 gennaio 2018—La vastità delle problematiche rivelate dal bug delle CPU Intel ed AMD (ma non delle ARM7!) ha in parte sorpreso anche Cassandra, che pure sul tema della inutile e pericolosa complessità dell'informatica già si era espressa qui e qui un decennio or sono.

Pochi se ne sono resi conto, ma il **bug rilevato nella maggior parte del silicio esistente** al mondo è di tipo particolarmente benigno, visto che compromette "solo" la riservatezza dei dati processati dalla maggioranza delle CPU esistenti, e "solo" se un attaccante ha raggiunto un accesso locale al computer.

Quello che mozza il respiro di chi ha orecchie per intendere e fantasia per estrapolare il futuro è la vastità e la pericolosità di questa classe di problemi, non più teorici od ipotizzati ma dimostrati.

Un esempio per tutti; per trasformare un problema globale ma limitato come Metdown in un incubo, basterebbe trovare il modo non di leggere ma di corrompere la memoria del kernel, mandando così in crash il computer?

Che potenza avrebbe una **cyber-arma** contenete un tale "zero-day del silicio" se potesse essere sfruttata per **mandare in crash tutte le CPU** di un paese nemico, o magari del mondo?

Basterebbe utilizzarla usando come vettore una botnet esistente, od un malware a diffusione rapida come l'ormai antico SQL-slammer; la fine del cyberspazio del nemico, o di tutto il cyberspazio, in un'unica, rapida mossa.

Il problema di fondo è comunque ancora più preoccupante; la società moderna fa **sempre più affidamento sulla tecnologia**, senza preoccuparsi nemmeno teoricamente dei rischi di catastrofi note quando si manifestassero con dimensioni enormi ma bassa probabilità, eventi chiamati in letteratura cigni neri (cfr. Nassim Nicholas "The Black Swan: The Impact Of The Highly Improbable" 2008).

Tantomeno si preoccupa di quello di catastrofi sconosciute ed imprevedibili, oltreché enormi, in gergo doppi cigni neri (cfr. Maurizio Barbeschi e Paolo Mastrolilli—"Fare i conti con l'ignoto. Governare l'incertezza: epidemie improvvise, catastrofi naturali, attentati terroristici"—2016).

Eppure il problema del "bug di silicio", pur così pubblicizzato dai media, potrebbe addirittura essere controproducente per un aumento della consapevolezza di questi problemi; tra qualche settimana, quando la notizia dal punto di vista mediatico sarà dimenticata, e nulla di grave sarà successo, tutto sembrerà tranquillo, e la gente, dai semplici utenti fino ai grandi produttori di hardware, ricomincerà a vivere come sempre ed a fare "business as usual".

Il **pericolo globale** da cui guardarsi non è un semplice silicio malprogettato, il problema vero è l'aumento continuo della complessità di qualsiasi oggetto tecnologico, che lo porta oltre la comprensione, sempre più limitata, dei suoi stessi progettisti.

Questo è aggravato dall'omogeneizzazione tecnologica che spinge, per motivi prevalentemente economici, verso l'adozione di piattaforme hardware e software sempre più simili che, come nel caso dell'omogeneità del genoma delle colture in campo biologico, può essere foriera di catastrofi causate da un singolo problema tecnico, come da un singolo parassita resistente.La gestione e limitazione della complessità, unita al controllo dell'eccessiva omogeneizzazione tecnologica delle infrastrutture, particolarmente di quelle critiche, è l'unica cosa che può scongiurare doppi cigni neri tecnologici.

Non bisogna permettere di usare un robot con un piede grosso come fermaporta solo perché costa poco, così come non si può usare un pc per visualizzare una singola lettera su uno schermo LCD; ambedue i sistemi prima o poi falliranno perché sono troppo complessi per la semplice funzione che devono fornire.

Ma il **fallimento nella funzione primaria**, anche se fosse catastrofico, sarebbe "solo" un cigno nero.

Un fallimento tecnologico imprevisto, come quello di un ipotetico "bug di silicio che resetti le CPU" sarebbe un doppio cigno nero, con conseguenze sia inattese che imprevedibili, praticamente illimitato nei danni che potrebbe provocare, specialmente se usato volontariamente come cyber-arma.

Sarebbe oltremodo opportuno che chi maneggia soldi pubblici o gestisce i budget di ricerca e sviluppo dei produttori di tecnologia, cominciasse a dar lavoro a chi si occupa di teoria delle catastrofi, di Analisi della complessità e di altre branche oggi marginali della fisica e della teoria dei sistemi per progettare tecnologie meno vulnerabili ed instabili, ed analizzare le possibili conseguenze di quelle già oggi esistenti e diffuse.

E che chiunque, ogni tanto, si fermasse un attimo nella vita frenetica che tutti conduciamo e si chiedesse "Se quello che sto usando cessasse di funzionare od addirittura scomparisse"?Cominciando dall'acqua del rubinetto, continuando con il silicio che permea ormai la nostra vita e proseguendo con gli annunci dei nuovi doni che le future tecnologie ci porteranno… doni forse di legno e con la forma di cavallo.

Originally published at punto-informatico.it.

By Marco A. L. Calamari on January 31, 2019.

Canonical link

Exported from Medium on August 27, 2025.